Claims

1. A method, for use in a virus-free certificate authority (102), of generating a virus-free certificate (200) certifying that a file is virus-free comprising the steps of:

- receiving (300) a virus-free certificate request for a file from a server (101) or a client (100) system, said virus-free certificate request comprising the file for which the virus-free certificate is requested;
- determining (301) whether a virus-free certificate is integrated in the file;

If no virus-free certificate is integrated in the file:

- determining (305) whether the file is virus-free or not;

if the file is declared virus-free by the virus-free certificate authority (102):

- generating (313, 314) a virus-free certificate (200) comprising a file signature (207) for certifying that said file is declared virus-free by the virus-free certificate authority (102);
- integrating (316) the generated virus-free certificate (200) in the file;
- sending (316) back in response to the virus-free certificate request the file with the integrated virus-free certificate (200).

2. The method according to ~~the preceding~~ claim *1* wherein the virus-free certificate request comprises:

- a list of one or a plurality of anti-virus programs to execute on the file to determine whether the file is virus-free or not.

3. The method according to ~~any one of the preceding~~ claims *1* wherein said file comprised in the virus-free certificate request comprises:

- an integrated virus-free certificate.

FR 9 99 116/YNE

34. The method according to ~~any one of the preceding~~ claim **1** comprising the further steps of:

If the file comprises an integrated virus-free certificate:

- determining (302, 303) whether the virus-free certificate integrated in the file has been previously generated by the virus-free certificate authority.

If the virus-free certificate integrated in the file has been previously generated by the virus-free certificate authority:

- updating (304) the virus-free certificate.

If the virus-free certificate integrated in the file has not been previously generated by the virus-free certificate authority:

- generating (313, 314) a new virus-free certificate.

5. The method according to ~~any one of the preceding~~ claim **1** wherein said file further comprises:

- a file header comprising:
- a non encrypted file signature (501);
- a file length (502);
- a product name (503).

6. The method according to ~~any one of the preceding~~ claim **1** wherein said step of integrating (316) the virus-free certificate (200) in the file comprises the further steps of:

- appending (506) the virus-free certificate to the file;
- modifying ~~the~~ **a** file header, preferably:
- ~~the~~ **a** non encrypted file signature (501);
- ~~the~~ **a** file length (502);
- ~~the~~ **a** product name (503), said product name comprising means for identifying the integrated virus-free certificate.

FR 9 99 116/YNE

7. The method according to ~~any one of the preceding~~ claims wherein said step of determining whether the file is virus-free or not comprises the further step of:

* executing (301) one or a plurality of anti-virus programs on said file for detecting viruses.

8. The method according to ~~any one of the preceding~~ claims wherein the virus-free certificate further comprises:

* ~~the~~ a list of the one or plurality of anti-virus programs (208) that have been executed on the file.

9. The method according to ~~any one of the preceding~~ claims wherein the virus-free certificate (200) further comprises:

* a file identification (201);
* a virus-free certificate authority identification (202);
* a public key (203) for decrypting the file signature;
* a certificate signature (206) for authenticating the virus-free certificate.

10. The method according to ~~any one of the preceding~~ claims comprising the further steps (305) of:

* identifying the server (101) or client (100) system where the file comprising the integrated virus-free certificate is stored;
* updating the file with the integrated virus-free certificate.

11. The method according to ~~any one of the preceding~~ claims wherein the step of generating (303, 304) a file signature (207) comprises the further steps of:

FR 9 99 116/YNE

- hashing the file to generate a file digest;
- encrypting the file digest using a private key.

12. A system, preferably a virus-free certificate authority (102), for carrying out the method according to any one of the preceding claims.

13. A computer program comprising instructions for carrying out the method according to any one of claims 1 to 11.

14. A method, for use in a server (101) or client (100) system, of determining that a file is virus-free comprising the steps of:

- determining (401) whether a virus-free certificate (200) is integrated within a file; if a virus-free certificate is integrated within the file:
- authenticating (415) the virus-free certificate (200), said virus-free certificate comprising a certificate signature (206);
- authenticating (407) the file, said virus-free certificate (200) comprising a file signature (207), said file signature certifying that said file has been declared virus-free by a virus-free certificate authority (102).

15. The method according to ~~the preceding~~ claim 14 wherein said step of authenticating (407) the file comprises the further steps of:

- decrypting the file signature (207) using a public key (203) comprised in the virus-free certificate (200).
- hashing the file to generate a file digest;
- comparing the decrypted file signature with the generated file digest.

FR 9 99 116/YNE

16. The method according to ~~any one of~~ claims 14 ~~to 15~~ wherein the step of authenticating the virus-free certificate comprises the further step of:

• validating the virus-free certificate.

17. The method according to ~~any one of~~ claims 14 ~~to 16~~ wherein the step of validating the virus-free certificate comprises the further step of:

• determining whether the virus-free certificate is valid or not;

If the virus-free certificate is not valid:

• requesting a virus-free certificate update or an updated virus-free certificate update to a virus-free certificate authority (102).

18. The method according to ~~any one of the~~ claims 14 ~~to 17~~ wherein the virus-free certificate (200) further comprises:

• a file identification (201);

• a virus-free certificate authority identification (202);

• a public key (203) for decrypting the file signature;

19. The method according to ~~any one of~~ claims 14 ~~to 18~~ wherein said file further comprises:

• a file header comprising:

• a non encrypted file signature (501) for signing the file;

• a file length (502);

• a product name (503), said product name comprising means for identifying the integrated virus-free certificate.

FR 9 99 116/YNE

20. The method according to ~~any one of~~ claims 14 ~~to 19~~ wherein the step of determining (401) whether a virus-free certificate (200) is integrated within a file comprises the further step of:

- determining whether a product name (503) within the file header comprises means for identifying the integrated virus-free certificate or not.

21. A system, preferably a server (101) or client (100) system, for carrying out the method according to any one of claims 14 to 20.

22. A computer program comprising instructions for carrying out the method according to any one of claims 14 to 20.

FR 9 99 116/YNE